ABSTRACT

A cipher text supplying configuration applying a tree structure and based on a CS scheme is provided, which enables a reduction of the amount of information to be stored in and the amount of calculation to be performed by, equipment that execute decryption of a cipher text. A Rabin Tree is generated as a one-way tree in which node-corresponding values are set so as to correspond to nodes constituting a hierarchical tree. A node-corresponding value NV_a is set so as to be calculable by application of a function f based on a node-corresponding value NV_b and a node-added variable $salt_b$ set so as to correspond to at least one lower-rank node. Thus, it is configured such that a node key NK is calculable by application of a function Hc with node-corresponding values NV corresponding to nodes as inputs. As a result of the present configuration, the amount of information required for a receiver to be held safely can be reduced, and also, the amount of calculation required for node key calculation can be reduced, whereby a secure cipher text distribution and decryption processing configuration is implemented.